P14683-A

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　１月１２日

出願番号
Application Number: 特願２００１－００５００２

出願人
Applicant(s): 日本電信電話株式会社

２００１年　６月１３日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０５５４３４

【書類名】　特許願

【整理番号】　NTTH126778

【提出日】　平成13年 1月12日

【あて先】　特許庁長官殿

【国際特許分類】　G06K 9/00

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　重松　智志

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　森村　浩季

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　町田　克之

【特許出願人】

【識別番号】　000004226

【氏名又は名称】　日本電信電話株式会社

【代理人】

【識別番号】　100064621

【弁理士】

【氏名又は名称】　山川　政樹

【電話番号】　03-3580-0961

【手数料の表示】

【予納台帳番号】　006194

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9701512

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　認証トークンおよび認証システム

【特許請求の範囲】

【請求項１】　通常時はユーザにより所持されるとともに、そのユーザの認証データに応じて所定の処理を行う利用機器をユーザが利用する場合には、その利用機器へ接続されて前記ユーザの生体情報に基づきユーザ認証を行う認証トークンであって、

前記ユーザの生体情報を検出しその検出結果をセンシングデータとして出力するセンサと、

前記ユーザの生体情報を照合するための登録データが予め格納されている記憶回路と、

前記記憶回路に記憶されている登録データを用いて前記センサからのセンシングデータを照合し、ユーザ認証結果を示すその照合結果を認証データとして出力する照合回路と、

この照合回路からの認証データを通信データとして前記利用機器へ送信する通信回路とが、一体に形成されていることを特徴とする認証トークン。

【請求項２】　請求項１記載の認証トークンにおいて、

前記記憶回路は、前記利用機器での処理に用いられる前記ユーザに固有のユーザ情報を予め記憶し、

前記照合回路は、前記記憶回路から読み出した前記ユーザ情報を前記認証データに含めて出力することを特徴とする認証トークン。

【請求項３】　請求項１または２記載の認証トークンにおいて、

前記通信回路からの通信データを所定のデータ形式へ変換して前記利用機器へ送信するプロトコル変換回路をさらに備えることを特徴とする認証トークン。

【請求項４】　請求項１または２記載の認証トークンにおいて、

前記通信回路からの通信データを無線区間を介して前記利用機器へ送信する無線回路をさらに備えることを特徴とする認証トークン。

【請求項５】　請求項３記載の認証トークンにおいて、

前記プロトコル変換回路からの通信データを無線区間を介して前記利用機器へ

送信する無線回路をさらに備えることを特徴とする認証トークン。

【請求項６】　請求項１～５記載の認証トークンにおいて、

当該認証トークン内へ電源供給を行う電池をさらに備えることを特徴とする認証トークン。

【請求項７】　請求項６記載の認証トークンにおいて、

前記電池は、当該認証トークンが前記利用機器へ接続された際にその利用機器からの電源供給により充電される二次電池からなることを特徴とする認証トークン。

【請求項８】　所定の処理を行う利用機器を利用する場合に必要なユーザ認証をユーザの生体情報を用いて行う認証システムであって、

通常時はユーザにより所持されるとともに、ユーザが前記利用機器を利用する場合はその利用機器へ接続されて前記ユーザの生体情報に基づきユーザ認証を行う認証トークンを備え、

前記認証トークンは、前記ユーザの生体情報を検出しその検出結果をセンシングデータとして出力するセンサと、前記ユーザの生体情報を照合するための登録データが予め格納されている記憶回路と、前記記憶回路に記憶されている登録データを用いて前記センサからのセンシングデータを照合し、ユーザ認証結果を示すその照合結果を認証データとして出力する照合回路と、この照合回路からの認証データを通信データとして前記利用機器へ送信する第１の通信回路とを有するとともに、これら回路部が一体として形成されており、

前記利用機器は、前記認証トークンから送信された通信データを受信し認証データとして出力する第２の通信回路と、この第２の通信回路からの認証データに含まれる照合結果に基づき前記所定の処理を行う処理回路とを備えることを特徴とする認証システム。

【請求項９】　請求項８記載の認証システムにおいて、

前記認証トークンの記憶回路は、前記利用機器での処理に用いられる前記ユーザに固有のユーザ情報を予め記憶し、

前記認証トークンの照合回路は、前記記憶回路から読み出した前記ユーザ情報を前記認証データに含めて出力し、

前記利用機器の処理回路は、前記第２の通信回路からの認証データに含まれるユーザ情報を用いて処理を行うことを特徴とする認証システム。

【請求項１０】　請求項８または９記載の認証システムにおいて、

前記認証トークンに接続され、前記認証トークンの前記第１の通信回路からの通信データを所定のデータ形式へ変換して前記利用機器へ送信するデータ変換モジュールをさらに備えることを特徴とする認証システム。

【請求項１１】　請求項８または９記載の認証システムにおいて、

前記認証トークンに接続され、前記認証トークンの前記第１の通信回路からの通信データを無線区間を介して前記利用機器へ送信する無線モジュールをさらに備え、

前記利用機器は、前記無線モジュールから送信された前記通信データを無線区間を介して受信し前記第２の通信回路へ出力する無線回路を有することを特徴とする認証システム。

【請求項１２】　請求項１０記載の認証システムにおいて、

前記認証トークンに接続され、前記データ変換モジュールからの通信データを無線区間を介して前記利用機器へ送信する無線モジュールをさらに備え、

前記利用機器は、前記無線モジュールから送信された前記通信データを無線区間を介して受信し前記第２の通信回路へ出力する無線回路を有することを特徴とする認証システム。

【請求項１３】　請求項８または９記載の認証システムにおいて、

前記認証トークンは、当該認証トークン内へ電源供給を行う電池をさらに有することを特徴とする認証システム。

【請求項１４】　請求項１０または１２記載の認証システムにおいて、

前記データ変換モジュールは、当該データ変換モジュール内および前記認証トークンへ電源供給を行う電池をさらに有することを特徴とする認証システム。

【請求項１５】　請求項１１または１２記載の認証システムにおいて、

前記無線モジュールは、当該無線モジュール内および前記認証トークンへ電源供給を行う電池をさらに有することを特徴とする認証システム。

【請求項１６】　請求項１３～１５記載の認証システムにおいて、

前記電池は、前記認証トークンが前記利用機器へ接続された際にその利用機器からの電源供給により充電される二次電池からなることを特徴とする認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、認証トークンおよび認証システムに関し、特に人間の生体情報を用いてユーザ本人であることを認証するための認証トークンおよび認識システムに関するものである。

【０００２】

【従来の技術】

高度情報化社会では、情報処理との親和性を持って厳密にユーザ本人を認証したいという要求が高い。特に、予め承認したユーザだけに入室を許可する入室管理システムや個人情報などの重要な情報を扱うような情報管理システム、あるいは電子決済を行う決済システムなどでは、上記のような要求が極めて高い。

このような要求に対し、半導体装置の製造技術や情報処理技術をベースとして、電子的に検出した固有の生体情報に基づきユーザ本人を認証するための認証システムの研究が盛んに行われている。

【０００３】

従来、このような認証システムは、図４に示すような構成となっていた。図４に従来の認証システムのブロック図を示す。

この認証システムでは、例えばユーザ認証が得られた場合に処理装置８４で所定のサービスを提供する利用機器８内に、センサ８１、記憶回路８２および照合回路８３が設けられている。センサ８１では指紋などの生体情報を電子的に検出し、得られたセンシングデータ８１Ａを照合回路８３へ出力する。一方、記憶回路８２にはユーザの生体情報を照合するための情報が登録指紋データ８２Ａとして記憶されている。

【０００４】

照合回路８３では、記憶回路８２から読み出した登録指紋データ８２Ａを用い

てセンサ８１からのセンシングデータ８１Ａを照合することにより、ユーザ認証を行う。そして、その認証結果を認証データ８３Ａとして処理装置８４へ出力する。処理装置８４では、照合回路８３からの認証データ８３Ａが認証成功を示す場合にのみ、所定のサービスをユーザに対して提供する。

また、図５に示すように、記憶回路８２のみを所持可能なデータカード９へ分離したものも考えられる。この場合には、サービス提供時、個々のユーザが所持するデータカード９が利用機器８へ接続され、利用機器８内に設けられた通信回路８５を介して、記憶回路８２に記憶されている登録指紋データ８２Ａが登録指紋データ８５Ａとして照合回路８３へ読み込まれて照合される。

【０００５】

【発明が解決しようとする課題】

しかしながら、このような従来の認証システムでは、ユーザの生体情報を検出するセンサ８１や照合を行う照合回路８３を利用機器８内部に設け、ユーザの生体情報を照合するための情報すなわち登録指紋データ８２Ａを用いて照合を行うものとなっているため、次のような問題点があった。

まず、前者（図４参照）によれば、①利用機器８内部の記憶回路８２にユーザの登録指紋データ８２Ａが予め登録されていないと、ユーザはたとえ本人であってもサービスを受けることは不可能である。また、②サービスを提供する全機器に多数ユーザの登録指紋データを記憶させるには、その配信方法や記憶方法が複雑かつ大規模になり、そのためコストの増加や安全性の低下を招いてしまう。さらに、③機器に自分の指紋データが登録されているのは、ユーザのプライバシー問題も引き起こし、心理的にも受け入れがたいシステムになってしまう。

【０００６】

これに対し、後者（図５参照）の認証システムでは、ユーザの登録データをデータカード９でユーザ自身が所持し管理するため、上記①～③の問題は回避できるが、④照合時にはユーザの登録指紋データがサービス機器に送信されるため、そのデータ漏洩に対する対策が必要であり、システムの規模が大きくなってしまう。さらに、⑤生体情報を検出するセンサ８１が不特定多数のユーザ間で共有しているため、センサ８１の故障時にはその機器に対するサービスが全て利用でき

なくなってしまう。また、⑥指紋などのようにセンサに対して人体の一部を接触させる必要がある場合は、センサ８１の共用によりユーザに対する衛生面でも問題があり、これらを解決するためにはシステムの規模が増大してしまう。

本発明はこのような課題を解決するためのものであり、照合時に用いる登録データの漏洩を防止でき、またセンサ故障による影響を最小限にとどめ、さらにはユーザに対して良好な衛生環境を保つことができる認証システムを提供することを目的としている。

【０００７】

【課題を解決するための手段】

このような目的を達成するために、本発明にかかる認証トークンは、通常時はユーザにより所持されるとともに、そのユーザの認証データに応じて所定の処理を行う利用機器をユーザが利用する場合には、その利用機器へ接続されてユーザの生体情報に基づきユーザ認証を行う認証トークンであって、ユーザの生体情報を検出しその検出結果をセンシングデータとして出力するセンサと、ユーザの生体情報を照合するための登録データが予め格納されている記憶回路と、記憶回路に記憶されている登録データを用いてセンサからのセンシングデータを照合し、ユーザ認証結果を示すその照合結果を認証データとして出力する照合回路と、この照合回路からの認証データを通信データとして利用機器へ送信する通信回路とを一体に形成したものである。

【０００８】

この場合、認証トークンの記憶回路で、利用機器での処理に用いられるユーザに固有のユーザ情報を予め記憶しておき、照合回路で、記憶回路から読み出したユーザ情報を認証データに含めて出力するようにしてもよい。

また、データ形式が異なる各種利用機器に対応するため、認証トークンの第１の通信回路からの通信データを所定のデータ形式へ変換して利用機器へ送信するプロトコル変換回路を設けてもよい。さらに、利用機器と無線区間を介して接続するため、認証トークンの第１の通信回路からの通信データあるいはプロトコル変換回路からの通信データを無線区間を介して利用機器へ送信する無線回路を設けてもよい。

また、認証トークン内に電池を設け、当該認証トークン内へ、具体的にはセンサ、記憶回路、照合回路および通信回路へ、さらにはプロトコル変換回路や無線回路へ電源供給を行うようにしてもよい。この電池として二次電池を用い、当該認証トークンが利用機器へ接続された際にその利用機器からの電源供給により充電するようにしてもよい。

【０００９】

また、本発明にかかる認証システムは、所定の処理を行う利用機器を利用する場合に必要なユーザ認証をユーザの生体情報を用いて行う認証システムであって、通常時はユーザにより所持されるとともに、ユーザが利用機器を利用する場合はその利用機器へ接続されてユーザの生体情報に基づきユーザ認証を行う認証トークンを備え、認証トークンに、ユーザの生体情報を検出しその検出結果をセンシングデータとして出力するセンサと、ユーザの生体情報を照合するための登録データが予め格納されている記憶回路と、記憶回路に記憶されている登録データを用いてセンサからのセンシングデータを照合し、ユーザ認証結果を示すその照合結果を認証データとして出力する照合回路と、この照合回路からの認証データを通信データとして利用機器へ送信する第１の通信回路とを設けてこれら回路部を一体として形成し、利用機器に、認証トークンから送信された通信データを受信し認証データとして出力する第２の通信回路と、この第２の通信回路からの認証データに含まれる照合結果に基づき所定の処理を行う処理回路とを設けたものである。

【００１０】

この場合、認証トークンの記憶回路で、利用機器での処理に用いられるユーザに固有のユーザ情報を予め記憶しておき、照合回路で、記憶回路から読み出したユーザ情報を認証データに含めて出力し、利用機器の処理回路で、第２の通信回路からの認証データに含まれるユーザ情報を用いて処理を行うようにしてもよい。

また、データ形式が異なる各種利用機器に対応するため、認証トークンの第１の通信回路からの通信データを所定のデータ形式へ変換して利用機器へ送信するデータ変換モジュールを認証トークンに接続して用いるようにしてもよい。さら

に、利用機器と無線区間を介して接続するため、認証トークンの第１の通信回路からの通信データを無線区間を介して利用機器へ送信する無線モジュールを認証トークンに接続して用い、また利用機器に、無線モジュールから送信された通信データあるいはデータ変換モジュールからの通信データを無線区間を介して受信し第２の通信回路へ出力する無線回路を設けるようにしてもよい。

【００１１】

また、認証トークンに電池を設け、その電池から認証トークン内へ電源供給を行うようにしてもよく、さらにデータ変換モジュールや無線モジュールへも電源供給するようにしてもよい。また、データ変換モジュールや無線モジュールに電池を設け、当該モジュールおよび認証トークンへ電源供給を行うようにしてもよい。

また、これら電池として二次電池を用い、当該認証トークンが利用機器へ接続された際にその利用機器からの電源供給により充電するようにしてもよい。

【００１２】

【発明の実施の形態】

次に、本発明の実施の形態について図面を参照して説明する。

図１は本発明の第１の実施の形態にかかる認証トークンおよびその認証トークンを用いた認証システムを示すブロック図である。

この認証システムは、ユーザ認証が得られた場合にサービスを提供する利用機器２と、通常時はユーザに所持されサービス提供時に利用機器２へ接続されてユーザの生体情報を用いたユーザ認証を行う認証トークン１とから構成されている。なお、本発明において、トークンとは、ユーザが所持し持ち運び可能な小型軽量の装置を指し、認証トークンとは、ユーザ本人の認証を行う機能を持つトークンをいう。以下では、生体情報として指紋を用いる場合を例として説明するが、生体情報としては、このほか声紋、虹彩、筆跡、手のひら形状（指の関節長）、静脈パターン、顔面配置パターンなどを用いることも可能である。

【００１３】

認証トークン１には、指紋（生体情報）を読み取るセンサ１１、ユーザ本人の登録指紋データ１２Ａやユーザ情報１２Ｂを記憶する記憶回路１２、センサ１１

での読み取り結果を示すセンシングデータ１１Ａを、記憶回路１２に記憶されている登録指紋データ１２Ａを用いて照合する照合回路１３、この照合回路１３での照合結果を含む認証データ１３Ａを通信データ１Ａとして認証トークン１の外部へ送信する通信回路１４が設けられており、これら回路部を一体として形成する認証トークン１が利用機器２に対して着脱自在に接続される。

利用機器２には、認証トークン１からの通信データ１Ａを受信する通信回路２１と、受信した通信データ１Ａに含まれる照合結果が一致を示す場合にのみ、そのユーザへのサービス提供を行う処理装置２２とが設けられている。

【００１４】

次に、図１を参照して、本実施の形態の動作について説明する。

ユーザは事前に、自分の所持する認証トークン１の記憶回路１２に、自分の登録指紋データ１２Ａやサービスを利用するためのパスワードや個人情報などからなるユーザ情報１２Ｂを記憶させておく。

利用機器２を利用する際、まずユーザは自分の認証トークン１を利用機器２へ接続し、指をそのセンサ１１へ置く。これにより認証トークン１のセンサ１１でユーザの指紋が読み取られセンシングデータ１１Ａとして出力される。このセンシングデータ１１Ａは照合回路１３において記憶回路１２の登録指紋データ１２Ａを用いて照合される。そして、その照合結果を含む認証データ１３Ａが出力される。このとき照合回路１３は、記憶回路１２に予め記憶回路１２に格納されているユーザＩＤ、パスワード、個人情報などのユーザ情報１２Ｂを読み出し、認証データ１３Ａへ含めて出力する。

【００１５】

通信回路１４では、照合回路１３からの認証データ１３Ａを通信データ１Ａとして利用機器２へ送信する。

利用機器２の通信回路２１では、認証トークン１の通信回路１４から送信された通信データ１Ａを受信し、認証データ１３と同じ内容の認証データ２１Ａとして出力する。処理装置２２では、この認証データ２１Ａを受け取ってその認証データ２１Ａに含まれる照合結果を参照する。そして、その照合結果が一致を示す場合、処理装置２２においてユーザの所望する所定の処理が実行される。

【００１６】

このように、本実施の形態では、ユーザの指紋を検出しその検出結果をセンシングデータとして出力するセンサ１１と、ユーザの指紋を照合するための登録指紋データ１２Ａが予め格納されている記憶回路１２と、この記憶回路１２に記憶されている登録指紋データ１２Ａを用いてセンサ１１からのセンシングデータ１１Ａを照合し、ユーザ認証結果となるその照合結果を認証データとして出力する照合回路１３と、この照合回路１３からの認証データを通信データ１Ａとして利用機器２へ送信する通信回路１４とを、認証トークン１として一体として形成したものである。

【００１７】

そして、認証に応じて所定の処理を行う利用機器２をユーザが利用する場合には、認証トークン１をその利用機器２へ接続し、その認証トークン１でユーザの生体情報に基づきユーザ認証を行い、利用機器２へ通知するようにしたものである。

また、利用機器２に、認証トークン１から送信された通信データ１Ａを受信し認証データ２１Ａとして出力する通信回路２１と、この通信回路２１からの認証データ２１Ａに含まれる照合結果に基づき所定の処理を行う処理装置２２とを設け、この利用機器２とは独立した各ユーザが個々の持つ認証トークン１での認証結果に基づき所定の処理を行うようにしたものである。

【００１８】

したがって、従来のように、ユーザの生体情報を検出するセンサや照合を行う照合回路を利用機器内部に設け、ユーザの登録データをデータカードでユーザ自身が所持し管理する場合と比較して、登録データが認証トークンの外部へ出力されることがなくなり照合時に用いる登録データの漏洩を防止できる。また、センサを不特定多数のユーザで共用する必要がなく、ユーザが個々に所持する認証トークンごとに設けられているセンサを用いるため、センサ故障が発生しても他のユーザには波及せず、さらに生体情報検出の際、指紋などのようにセンサに対して人体の一部を接触させる必要がある場合でもユーザに対して良好な衛生環境を保つことができる。

【００１９】

認証トークン１については、ユーザが所持するのに適するように、上記のセンサ、記憶回路および照合回路などの各種回路が一体に形成、すなわち同一の筐体に収容されている。この場合、これらの各種回路を同一基板上に形成してもよく、これらの各種回路を１チップの半導体装置として形成する技術（例えば、特開２０００－２４２７７１号公報など参照）を用いることで、非常に小型な認証トークンを実現することも可能となる。

【００２０】

さらに、記憶回路１２にユーザＩＤやパスワードさらには個人情報などのユーザ情報１２Ｂを予め記憶しておき、これらを認証データ１３Ａに含めて利用機器２へ送信するようにしたので、利用機器２の処理装置２２において、その認証データに含まれるユーザ情報１２Ｂ、例えばユーザＩＤやパスワードをチェックすることにより処理実行の可否を判断でき、利用機器で行う処理の重要性に合わせた基準で認証判定できる。また、ユーザ情報１２Ｂの個人情報、例えば氏名、住所、電話番号、口座番号やクレジットカード番号などを処理に用いることにより、処理に必要な個人情報をユーザが入力する必要がなくなり、ユーザの操作負担を大幅に軽減できる。

【００２１】

次に、図２を参照して、第２の実施の形態について説明する。図２は本発明の第２の実施の形態にかかる認証システムを示すブロック図である。本実施の形態は、上記第１の実施の形態の認証システム（図２参照）のうち、認証トークン１の出力段にデータ変換モジュール３を付加したものである。

このデータ変換モジュール３には、認証トークン１の通信回路１４から出力された通信データを、利用機器２で受信・解読可能なデータ形式へ変換するプロトコル変換回路３１が設けられている。

【００２２】

このように、認証トークン１に着脱自在に取り付けられるデータ変換モジュール３を介して、所望の利用機器２と認証トークン１とを接続するようにしたので、データ形式が異なる利用機器に対しても同一認証トークンを用いたユーザ認証

が可能となる。また、様々な形式に対応したデータ変換モジュールを用意し、それらを認証トークンに対して容易に着脱交換することで、ユーザが１つの認証トークンを用いて様々な利用機器を利用することができ、複数の認証トークンを所持する必要がない。また、１つのデータ変換モジュールを複数のユーザで共用することも可能である。

以上では、データ変換モジュール３を認証トークン１に対して着脱自在に取り付ける場合を例として説明したが、認証トークン１内部にプロトコル変換回路３１を設けてもよく、さらにコンパクトに構成できる。

【００２３】

次に、図３を参照して、第３の実施の形態について説明する。図３は本発明の第３の実施の形態にかかる認証システムを示すブロック図である。本実施の形態は、上記第１の実施の形態の認証システム（図１参照）のうち、認証トークン１の出力段に無線モジュール４を付加したものである。

この無線モジュール４には、認証トークン１の通信回路１４から出力された通信データを、利用機器２で受信・解読可能なデータ形式へ変換するプロトコル変換装置４１と、このプロトコル変換装置４１からの通信データを無線区間を介して利用機器２へ送信する無線回路４２とが設けられている。この場合、利用機器２側にも無線回路２３を設ける必要がある。

【００２４】

このように、認証トークン１に着脱自在に取り付けられる無線モジュール４を用いて、所望の利用機器２と認証トークン１とを接続するようにしたので、ユーザは、認証トークン１を利用機器２に直接接続することなく、例えば自分の手元で認証トークン１を用いてユーザ認証を行いサービスを受けることが可能となる。したがって、利用機器２に対して認証トークン１を接続する作業や、利用機器２に接続されている状態の認証トークン１を用いて認証を行う作業など、認証時のユーザに対する作業負担を大幅に軽減できる。

【００２５】

また、様々な通信プロトコルに対応した無線モジュールを用意し、それらを認証トークンに対して容易に着脱交換することで、ユーザが１つの認証トークンを

用いて様々な利用機器を利用することが可能となる。さらに、１つの無線モジュールを複数のユーザで共用することも可能である。

なお、利用機器２と認証トークン１の通信プロトコルが同一の場合は、無線モジュール４のプロトコル変換回路４１を省略することも可能である。また、無線回路４２の代わりに、赤外線通信回路や超音波通信回路など、無線区間を介してデータ通信可能な通信回路を用いてもよい。

以上では、無線モジュール４を認証トークン１に対して着脱自在に取り付ける場合を例として説明したが、認証トークン１内部に無線回路４２やプロトコル変換回路４１を設けてもよく、さらにコンパクトに構成できる。また、認証トークン１と利用機器２との間でやり取りする認証データや通信データに対して暗号化方式を用いてもよく、上記各実施の形態について適用できる。

【００２６】

以上で説明した第１～第３の実施の形態において、認証トークン１やデータ変換モジュール３、無線モジュール４への電力は、認証トークン内に設けた電池を用いて供給するようにしてもよい。また、認証トークン１が利用機器２に接続されている状態で、利用機器２内の電源から認証トークン１へ電源供給するようにしてもよい。このとき、認証トークン１内の電池として充電可能な二次電池を用い、利用機器２と接続状態にあるときに、利用機器２内の電源を用いてその二次電池を充電するようにしてもよい。

また、非接触カードなどで用いられる非接触電力供給技術を用いて、利用機器から認証トークン１やデータ変換モジュール３、無線モジュール４への電源供給や、二次電池の充電を行うようにしてもよい。

なお、認証トークン１に対する電力供給については、上記構成例に限定されるものではない。

【００２７】

以上で説明した第２の実施の形態において、データ変換モジュール３内に設けた電池を用いて、データ変換モジュール３や認証トークン１の各回路へ電力供給するようにしてもよい。また、このデータ変換モジュール３内の電池として充電可能な二次電池を用い、利用機器２の電源を用いてこの二次電池を充電するよう

にしてもよい。

以上で説明した第３の実施の形態において、無線モジュール４内に設けた電池を用いて、無線モジュール４や認証トークン１の各回路へ電源供給するようにしてもよい。また、この無線モジュール４内の電池として充電可能な二次電池を用い、利用機器２の電源を用いてこの二次電池を充電するようにしてもよい。

【００２８】

【発明の効果】

以上説明したように、本発明は、ユーザの生体情報を検出しその検出結果をセンシングデータとして出力するセンサと、ユーザの生体情報を照合するための登録データが予め格納されている記憶回路と、記憶回路に記憶されている登録データを用いてセンサからのセンシングデータを照合し、ユーザ認証結果を示すその照合結果を認証データとして出力する照合回路と、この照合回路からの認証データを通信データとして利用機器へ送信する通信回路とを、認証トークンとして一体に形成し、この認証トークンを通常時はユーザにより所持し、ユーザが利用機器を利用する場合はその利用機器へ接続してユーザの生体情報に基づきユーザ認証を行うようにしたものである。

【００２９】

したがって、従来のように、ユーザの生体情報を検出するセンサや照合を行う照合回路を利用機器内部に設け、ユーザの登録データをデータカードでユーザ自身が所持し管理する場合と比較して、登録データが認証トークンの外部へ出力されることがなくなり照合時に用いる登録データの漏洩を防止できる。また、センサが不特定多数のユーザで共用されず、ユーザが個々に所持する認証トークンごとに設けられているため、センサ故障が発生しても他のユーザには波及せず、さらに生体情報を検出する際に指紋などのようにセンサに対して人体の一部を接触させる必要がある場合でもユーザに対して良好な衛生環境を保つことができる。

【図面の簡単な説明】

【図１】　本発明の第１の実施の形態による認証トークンおよび認証システムを示すブロック図である。

【図２】　本発明の第２の実施の形態による認証トークンおよび認証システ

ムを示すブロック図である。

【図３】　本発明の第３の実施の形態による認証トークンおよび認証システムを示すブロック図である。

【図４】　従来の認証システムを示すブロック図である。

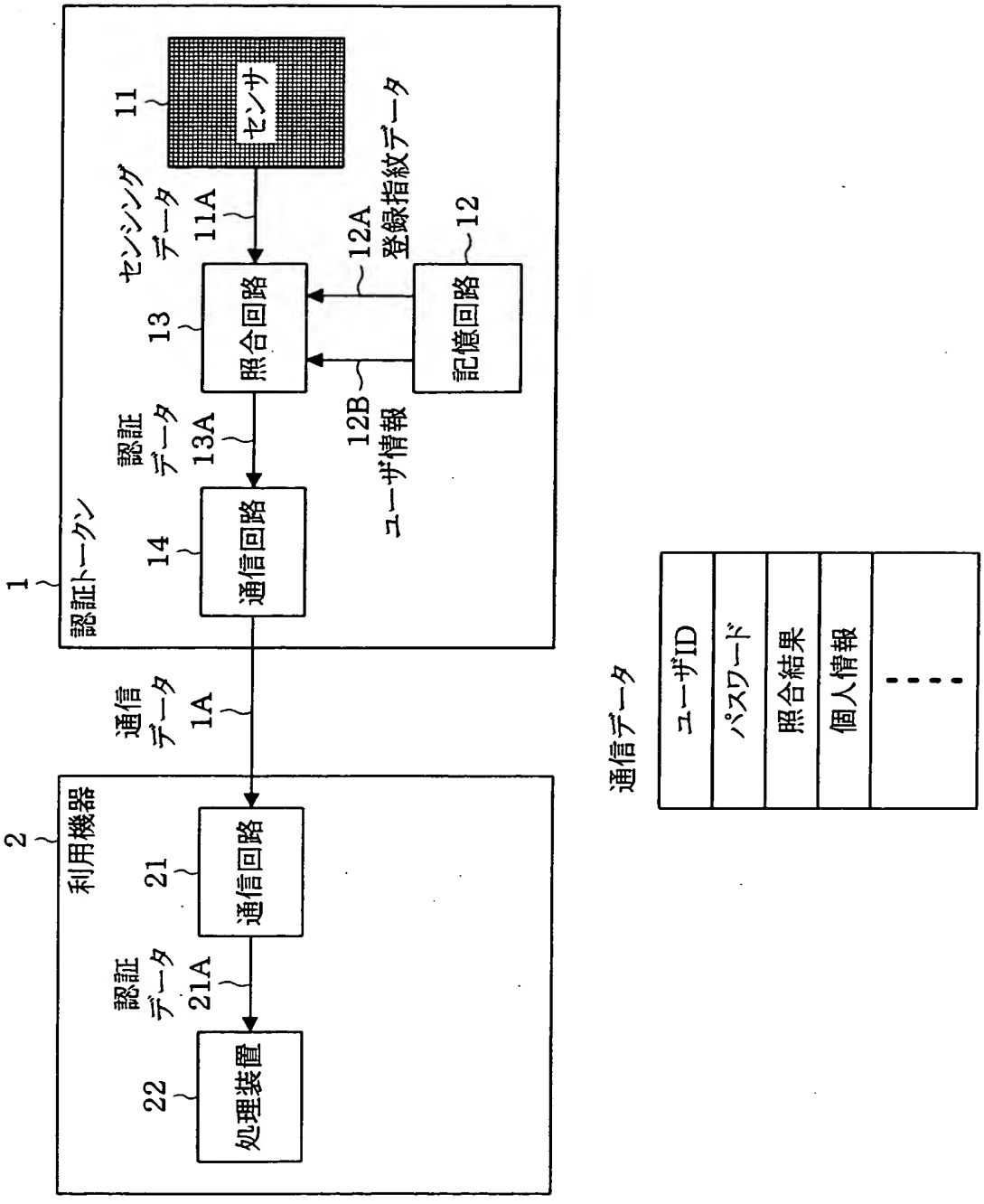
【図５】　従来の他の認証システムを示すブロック図である。

【符号の説明】

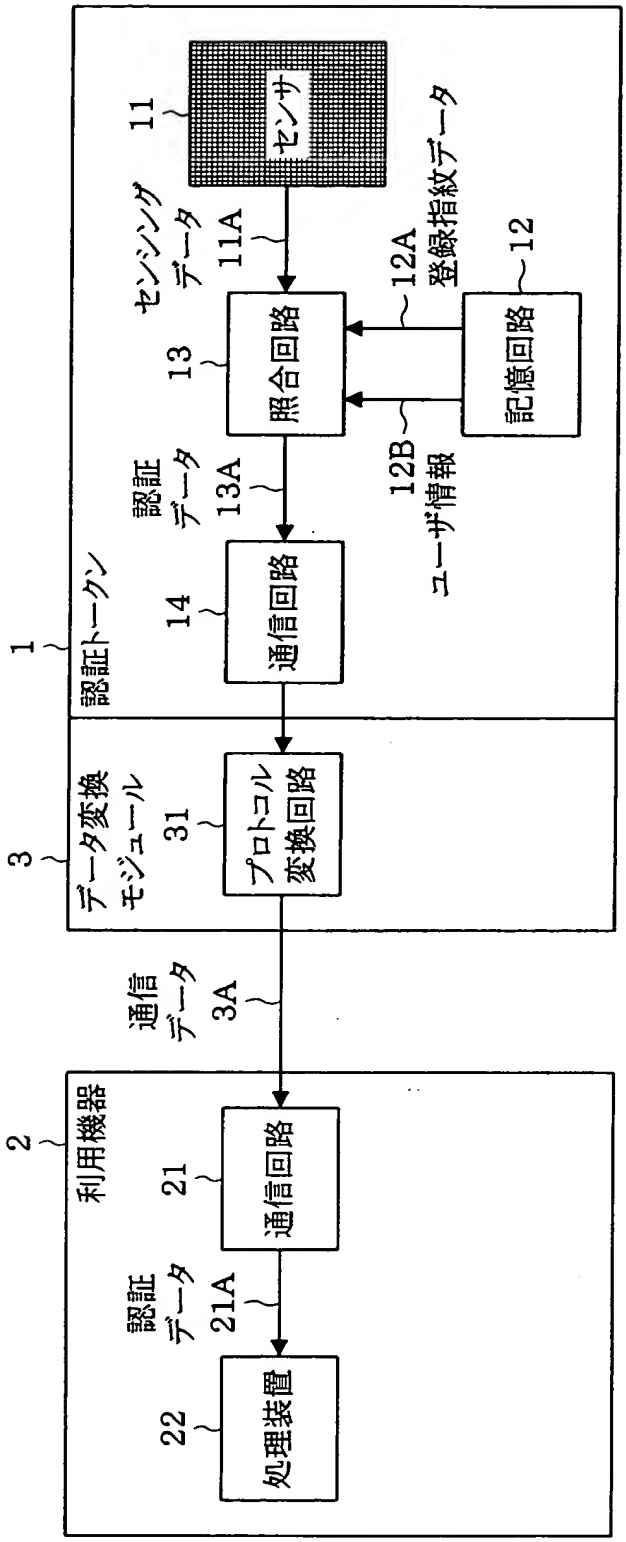
１…認証トークン、１１…センサ、１２…記憶回路、１２Ａ…登録指紋データ、１２Ｂ…ユーザ情報、１３…照合回路、１３Ａ…認証データ、１４…通信回路、１Ａ…通信データ、２…利用機器、２１…通信回路、２１Ａ…認証データ、２２…処理装置、２３…無線回路、３…データ変換モジュール、３１…プロトコル変換回路、３Ａ…通信データ、４…無線モジュール、４１…プロトコル変換回路、４２…無線回線、４Ａ…通信データ。

【書類名】　　図面

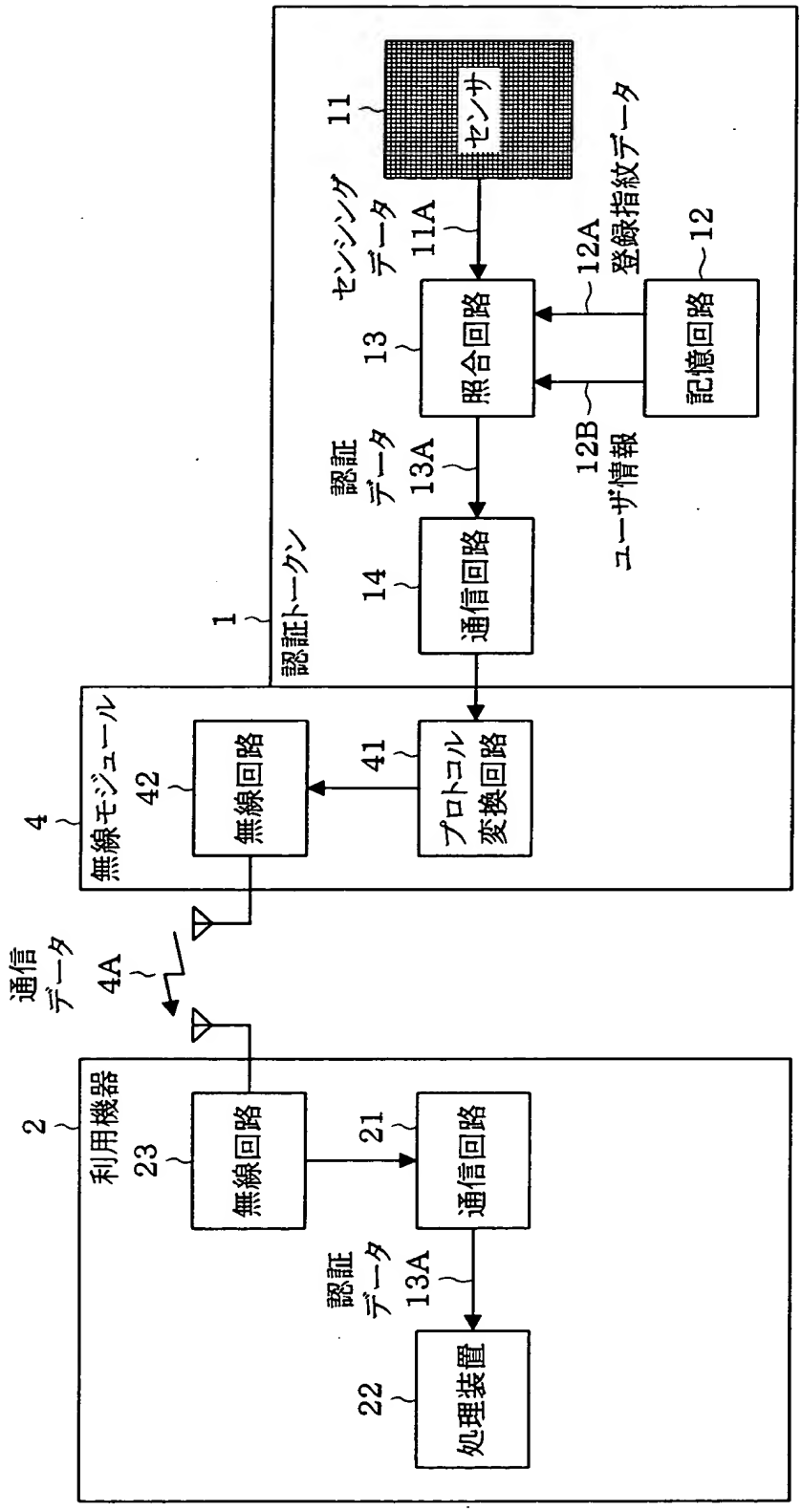
【図１】


1
認証トークン
センサ
11
センシングデータ
11A
照合回路
13
記憶回路
12
12A
登録指紋データ
12B
ユーザ情報
認証データ
13A
通信回路
14
通信データ
1A
2
利用機器
通信回路
21
認証データ
21A
処理装置
22
通信データ
ユーザID
パスワード
照合結果
個人情報

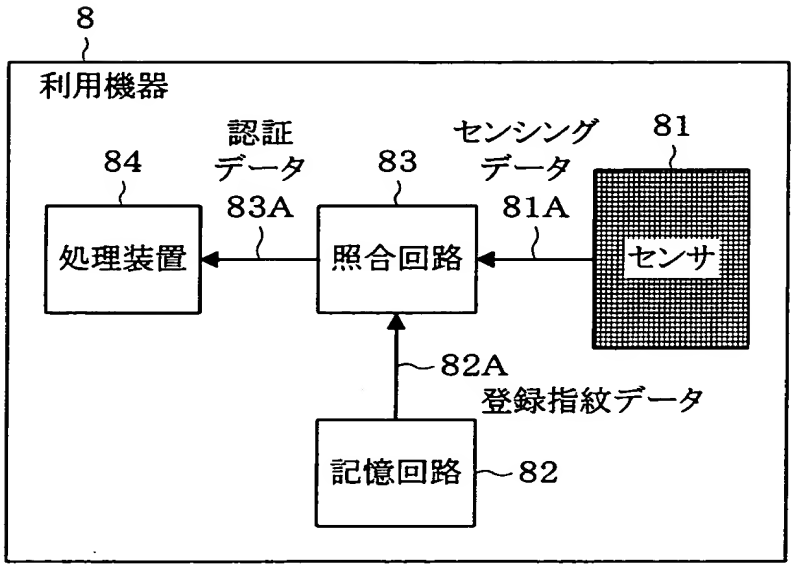
【図２】


1
認証トークン
センサ
11
センシングデータ
11A
照合回路
13
記憶回路
12
登録指紋データ
12A
ユーザ情報
12B
認証データ
13A
通信回路
14
3
データ変換モジュール
プロトコル変換回路
31
通信データ
3A
2
利用機器
通信回路
21
認証データ
21A
処理装置
22

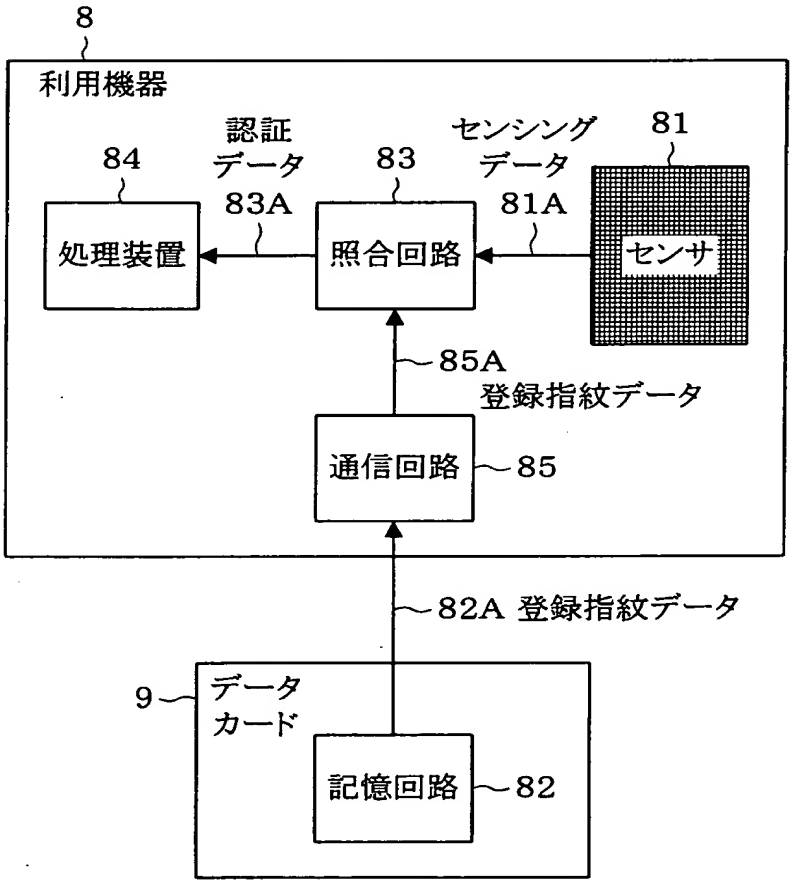
【図３】


認証トークン
1
センサ
11
センシングデータ
11A
登録指紋データ
12A
記憶回路
12
照合回路
13
ユーザ情報
12B
認証データ
13A
通信回路
14
無線モジュール
4
無線回路
42
プロトコル変換回路
41
通信データ
4A
利用機器
2
無線回路
23
通信回路
21
認証データ
13A
処理装置
22

【図４】


8
利用機器
認証
データ
センシング
データ
81
84
83
83A
81A
処理装置
照合回路
センサ
82A
登録指紋データ
記憶回路
82

【図５】


8
利用機器
認証
データ
センシング
データ
81
84
83
83A
81A
処理装置
照合回路
センサ
85A
登録指紋データ
通信回路
85
82A 登録指紋データ
9
データ
カード
記憶回路
82

【書類名】　　要約書

【要約】

【課題】　照合時に用いる登録データの漏洩を防止でき、またセンサ故障による影響を最小限にとどめ、ユーザに対して良好な衛生環境を保つようにする。

【解決手段】　認証トークン１では、センサ１１，記憶回路１２、照合回路１３および通信回路１４を一体として形成し、センサ１１によりユーザの指紋を検出しその検出結果をセンシングデータ１１Ａとして出力する。照合回路１３では、記憶回路１２に記憶されている登録指紋データ１２Ａを用いてセンサ１１からのセンシングデータ１１Ａを照合し、ユーザ認証結果を示すその照合結果を認証データとして出力し、この認証データを通信回路１４から通信データ１Ａとして前記利用機器２へ送信する。利用機器では、認証トークン１から通信データ１Ａとして受信した認証データに基づき所定の処理を実行する。

【選択図】　　図１

出 願 人 履 歴 情 報

識別番号　〔０００００４２２６〕

１．変更年月日　１９９９年　７月１５日
［変更理由］　住所変更
住　所　東京都千代田区大手町二丁目３番１号
氏　名　日本電信電話株式会社